WHAT IS CYBER PHYSICAL SYSTEMS SECURITY?

Cyber Physical Systems Security is protection for smart, connected technology such as sensors, processors or actuators that interact with the physical world. Examples of this technology, commonly known as the Internet of Things, include smart speakers in your kitchen, thermostats that self-learn and lighting that turns on or off when spoken to. This technology is also being integrated into our infrastructure, improving everything from power grids to food supplies to production lines.

The importance of keeping these new tools secure is obvious, especially when it comes to infrastructure — the backbone of our society. As many devices have rapidly come to market to meet demands, many users have been unknowingly put at risk. When it comes to power grids or water supplies, these points of failure can't be allowed.

Cyber Physical Systems Security provides total protection against this threat while denying our adversaries what they really want — to leverage our own resources against us and limit our response capabilities.

Internet-connected technology is changing our infrastructure for the better, from the national power grid to our transportation and agricultural systems. But if not properly protected, these important new tools can also pose great risks to our national security. Cyber Physical Systems Security helps to ensure the critical, smart systems that interact with the world — such as medical devices, manufacturing robots and irrigation controls — stay safe, secure and functioning.
Our Approach:
Raytheon’s history in secure, technical and complicated systems makes us the perfect partner to deliver Cyber Physical Systems Security. The company understands what it takes to be a large system integrator with years of delivering successful military, government and commercial solutions on no-fail, critical systems such as weapon systems or air traffic control management.

As one of the world’s biggest cybersecurity and defense companies, Raytheon approaches each challenge with the understanding that every organization has a different mission, need or problem to solve. In addition, we know that added security solutions must be designed to avoid unintended consequences to overall system performance. For example, security solutions for a smart power grid shouldn’t impinge functionality or cause new problems.

That’s why Raytheon’s experience and people-first approach stand out — we use our knowledge to ensure everyday operations aren’t affected by otherwise well-meaning solutions. We harden platforms and increase resiliency while detecting and preventing intrusions so that everything continues to function as it should.

With the right training, software, people, platforms and knowledge, Raytheon has the solutions to today’s and tomorrow’s physical cyber problems.

WHAT’S NEXT?
As smart devices and technology continue to proliferate and become integrated into all we do, there will be no resting when it comes to Cyber Physical Systems Security. Raytheon is working on technology enhancements to provide total security integration into all elements of a business’s operations. And with advancements in machine learning and artificial intelligence, our solutions will help identify faults through the use of predictive analytics, helping keep the security of our infrastructure one step ahead of those who would do it harm.